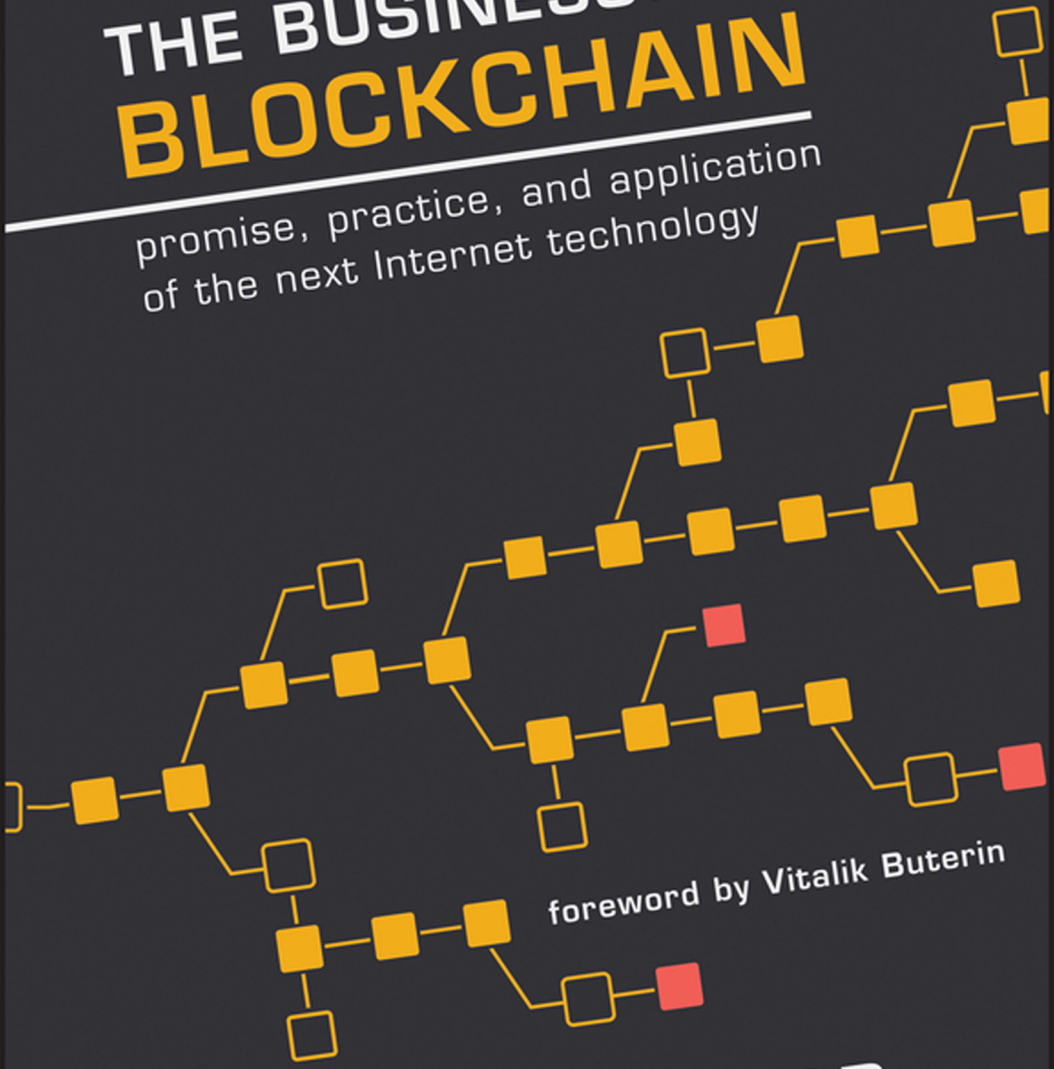
THE BUSINESS BLOCKCHAIN

promise, practice, and application of the next Internet technology



foreword by Vitalik Buterin

WILLIAM MOUGAYAR

Author of *Centerless*

WILEY

THE BUSINESS BLOCKCHAIN

THE BUSINESS BLOCKCHAIN

Promise, Practice, and Application of the Next Internet Technology

WILLIAM MOUGAYAR

FOREWORD BY VITALIK BUTERIN

Cover and book design: THE FRONTISPIECE

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

ISBN 978-1-119-30031-1 (cloth)
ISBN 978-1-119-30032-8 (ePDF)
ISBN 978-1-119-30033-5 (ePub)

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

For my parents, who
continue to be by my side.

To Maureen, with whom
everything is possible.

And to our beloved dog, Pasha,
the brave little Bichon Frisé.
You filled my heart forever.

CONTENTS

FOREWORD

THIS DECADE IS AN INTERESTING TIME for the development of decentralized technologies. Although cryptographers, mathematicians and coders have been working on increasingly specific and advanced protocols in order to get stronger and stronger privacy and authenticity guarantees out of various systems—from electronic cash to voting to file transfer—progress was slow for over 30 years. The innovation of the blockchain—or, more generally, the innovation of public economic consensus by Satoshi Nakamoto in 2009—proved to be the one missing piece of the puzzle that single-handedly gave the industry its next giant leap forward.

The political environment seemed to almost snap into place: the great financial crisis in 2008 spurred growing distrust in mainstream finance, including both corporations and the governments that are normally supposed to regulate them, and was the initial spark that drove many to seek out alternatives. Then Edward Snowden's revelations in 2013, highlighting how active the government was in realms citizens once believed private, were the icing on the cake. Even though blockchain technologies specifically have not seen mainstream adoption as a result, the underlying spirit of decentralization to a substantial degree has.

Applications ranging from Apple's phones to WhatsApp have started building in forms of encryption that are so strong that even the company writing the software and managing the servers cannot break it. For those who prefer corporations to government as

their boogeyman of choice, the advent of "sharing economy 1.0" is increasingly showing signs of failure to fulfill what many had originally seen to be its promise. Rather than simply cutting out entrenched and oligopolistic intermediaries, giants like Uber are simply replacing the middleman with themselves, and not always doing a better job of it.

Blockchains, and the umbrella of related technologies that I have collectively come to call "crypto 2.0," provide an attractive fix. Rather than simply hoping that the parties we interact with behave honorably, we are building technological systems that inherently build the desired properties into the system, in such a way that they will keep functioning with the guarantees that we expect, even if many of the actors involved are corrupt.

All transactions under "crypto 2.0" come with auditable trails of cryptographic proofs. Decentralized peer-to-peer networks can be used to reduce reliance on any single server; public key cryptography could create a notion of portable user-controlled identities. More advanced kinds of math, including ring signatures, homomorphic encryption, and zero-knowledge proofs, guarantee privacy, allowing users to put all of their data in the open in such a way that certain properties of it can be verified, and even computed on, without actually revealing any private details.

What is most surprising to early adopters of the technology, however, is just how rapidly institutional adoption has spread in the last two years. All the way from 2011 to 2013, the blockchain scene—or, realistically, what was then just the "bitcoin" scene—was very cryptoanarchist in spirit, with colorful and idealistic revolutionaries excited about "fighting the power" (or, more precisely, routing around the power). Today in 2016, however, the most exciting announcements all have to do with some collaboration announced with IBM or Microsoft, a research paper by the Bank of England, or a banking consortium announcing yet another round of new members.

What happened? In part, I would argue that the cryptoanarchists underestimated how flexible, technologically progressive, and even idealistic large corporations and banks can be. We often forget that corporations are made up of people, and people inside of corporations often have similar values and concerns to the kinds of regular people whom you might find at meetups. It might seem as though "the trust machine," as *The Economist* calls it, is purely a replacement for centralized anchors of trust, both in finance and elsewhere, that rely on real-world reputation and regulatory oversight, but the reality is much more complex. In truth, institutions do not fully trust one another either, and centralized institutions in one industry are just as concerned about centralization in other industries as regular people are. Energy companies, which are involved in producing and selling electricity, are just as happy to sell to a decentralized market as they are to a centralized one, and they may even prefer the decentralized version if it takes a smaller cut.

Furthermore, many industries are decentralized already, to an extent that many people outside of these industries do not appreciate, but they are decentralized in an inefficient way—a way that requires each company to maintain its own infrastructure around managing users, transactions, and data, and to reconcile with the systems of other companies every time it needs to interact. Consolidation around a single market leader would, in fact, make these industries more efficient. But neither the competitors of the likely leader nor antitrust regulators are willing to accept that outcome, leading to a stalemate. Until now. With the advent of decentralized databases that can technologically replicate the network effect gains of a single monopoly, everyone can join and align for their benefit, without actually creating a monopoly with all the negative consequences that it brings.

This is the story that arguably drives the interest in consortium chains in finance, blockchain applications in the supply chain industry, and blockchain-based identity systems. They all use

decentralized databases to replicate the gains of everyone being on one platform without the costs of having to agree on who gets to control that platform and then put up with them if they choose to try to abuse their monopoly position.

In the first four years after Satoshi's launch of Bitcoin in January 2009, much attention focused on the currency, including its payment aspects and its function as an alternative store of value. In 2013, attention started to shift to the "blockchain 2.0" applications: uses of the same technology that underlies Bitcoin's decentralization and security to other applications, ranging from domain name registration to financial contracts to crowdfunding and even games. The core insight behind my own platform, Ethereum, was that a Turing-complete programming language, embedded into the protocol at the base layer, could be used as the ultimate abstraction, allowing developers to build applications with any kind of business logic or purpose while benefiting from the blockchain's core properties. Around the same time, systems such as the decentralized storage platform InterPlanetary File System (IPFS) began to emerge, and cryptographers came out with powerful new tools that could be used in combination with blockchain technology to add privacy, particularly zk-SNARKs, or zero-knowledge Succinct Non-Interactive ARgument Knowledge. The combination of Turing-complete blockchain computing, non-blockchain decentralized networks using similar cryptographic technologies, and the integration of blockchains with advanced cryptography was what I chose to call "crypto 2.0"—a title that may be ambitious, but which I feel best captures the spirit of the movement in its widest form.

What is crypto 3.0? In part, the continuation of some of the trends in crypto 2.0, and particularly generalized protocols that provide both computational abstraction and privacy. But equally important is the current technological elephant in the room in the blockchain sphere: scalability. Currently, all existing blockchain

protocols have the property that every computer in the network must process every transaction—a property that provides extreme degrees of fault tolerance and security, but at the cost of ensuring that the network's processing power is effectively bounded by the processing power of a single node.

Crypto 3.0—at least in my mind—consists of approaches that move beyond this limitation, in one of various ways to create systems that break through this limitation and actually achieve the scale needed to support mainstream adoption (technically astute readers may have heard of "lightning networks," "state channels," and "sharding").

And then, there is also the question of adoption. Aside from the simple currency use case, "crypto 2.0" in 2015 saw a lot of people talking about it, developers releasing base platforms, but not yet any substantial applications. In 2016, we are seeing both startups and institutional players develop proof of concepts. Of course, the vast majority of these will never get anywhere and slowly wither away and die. That is inevitable in any field. It is a truism of entrepreneurship generally that 90% of all new businesses fail. But the 10% that succeed will likely at some point be scaled up into full-on products that reach millions of people—and that's where the fun really begins.

Perhaps William's book will inspire you to understand and, perhaps, join in refining the business blockchain.

Vitalik Buterin

Ethereum inventor and Chief Scientist,
Ethereum Foundation

APRIL 2, 2016

ACKNOWLEDGMENTS

SOME SAY WRITING A BOOK is a labor of love, and they are right. For me, it felt like assembling a puzzle on a canvas, then framing it.

Book writing is like an act of gift exchanging. The author spends an enormous amount of time to organize and concentrate their thoughts in writing. In return, readers donate their valuable time. Sometimes, a relationship develops between the author and readers. In my case, I welcome any reader who wishes to email me at wmougayar@gmail.com.

The moment I became involved in the blockchain industry, several people contributed to the shaping of my thinking and insights, but no single person had more influence on my education than Vitalik Buterin, creator and Chief Scientist at Ethereum. I am forever indebted to his time and knowledge, which he shared generously.

To all the creators, innovators, pioneers, leaders, entrepreneurs, startups, enterprise executives and practitioners who are living at the leading edges of this technological revolution, thank you for helping me connect the dots. You are the ones shining the lights ahead, despite some early pockets of darkness. My interactions with you have been invaluable. Thank you for allowing me a front seat, or backstage access to your wonderful acts.

At the risk of leaving some unnamed individuals in my professional circles, I would like to extend a very special gratitude to Muneeb Ali, Ian Allison,* Juan Benet, Pascal Bouvier,* Chris Allen, Jerry Brito, Anthony Di Iorio, Leda Glyptis, Brian Hoffman,* Andrew

Those indicated by asterik (*) were kind enough to review portions of the final manuscript.

Keys, Juan Llanos, Joseph Lubin, Adam Ludwin, Joel Monegro, Chris Owen, Sam Patterson, Denis Nazarov, Rodolfo Novak, Michael Perklin, Robert Sams,* Washington Sanchez, Amber Scott, Ryan Selkis, Barry Silbert, Ryan Shea, Ageesen Sri, Nick Sullivan, Nick Szabo, Tim Swanson, Simon Taylor,* Wayne Vaughan, Jesse Walden, Albert Wenger, Jeffrey Wilcke, Fred Wilson, and Gavin Wood. They all contributed, in different ways, to my understanding of Bitcoin, cryptocurrencies, blockchains, and their (decentralized) applications, either by teaching me, showing me, debating me, or allowing me into a piece of their world where I learned.

Special thanks to Wiley executive editor Bill Falloon, who believed we could do this faster than humanly possible, and to Kevin Barrett Kane at The Frontispiece who designed and produced the book in the nick of time.

Finally, much appreciation to the group of friends who helped support this book's Kickstarter campaign in February 2016, which made its production feasible. I could not have done this without you, and without the support of Margot Atwell and John Dimatos from Kickstarter.

One of a kind, Most Generous Supporter: Brad Feld (Foundry Group).

Really GENEROUS Supporters: Jim Orlando (OMERS Ventures), Ryan Selkis (DCG), Matthew Spoke (Deloitte).

Super SPECIAL Supporters: Kevin Magee, Piet Van Overbeke, Christian Gheorghe, Jon Bradford.

Super BIG Supporters: David Cohen (Techstars), Matthew Roszak (Bloq), Mark Templeton, Duncan Logan (RocketSpace), Michael Dalesandro.

BIG Supporters: Ahmed Alshaia, Floyd DCosta, Heino Døssing, Larry Erlich, Felix Frei, Jay Grieves, Emiel van der Hoek, Fergus Lemon, Amir Moulavi, Daniel A Greenspun, Michael O'Loughlin, Narry Singh, Amar Varma, Donna Brewington White, Neil Warren, Albert Wenger.

A PERSONAL PREFACE

I HAVE NOT ALWAYS BEEN SO LUCKY IN MANY THINGS, but one thing I lucked out on was my initial encounter with Vitalik Buterin, Ethereum's principal inventor who happened to be living in the same city as I did: Toronto.

On a cold early January 2014 evening, Vitalik came down the stairs at Bitcoin Decentral in an old narrow building on Spadina Avenue, an hour prior to the start of one of the weekly Toronto Bitcoin Meetups, organized by Anthony Di lorio. I spoke to him for the first time, trying to understand something that was described to me, as "beyond Bitcoin." For six months prior to that, I had been trying to understand Bitcoin, and this Ethereum technology was news to me.

Soon after my conversation started, the room was filling with people entering the building, ready for the Meetup to start. There was a special buzz around because Vitalik had just published his white paper[1] on a new blockchain platform that was supposed to be better than Bitcoin, and destined to become the next big thing.

Curious and intrigued, I proceeded to bombard Vitalik with questions about Ethereum and its architecture. I was impressed by his invention, but I was more interested in how it was going to be deployed. Vitalik didn't have all the answers. But he radiated a contagiously positive (yet slightly naive, at the time) determination and optimism about a better world out there. I sensed that this wasn't just about technology. It was more profound. It was

about society, government, business, old and new beliefs. It was about all of us. There was a human element to this technology that proposed more equitable solutions to our already complex and unjust world.

Two weeks later, I sat down with Vitalik and almost forced him to draw up an architecture of how Ethereum would work in the context of a deployment framework. I created my own hand drawn primitive version and showed it to him. He looked at it for three seconds, got agitated, opened Inkscape on his Windows PC, and frenetically started drawing the first version of a blockchain-based architectural framework with Ethereum in it. That architecture drawing was later iterated upon, and appeared in one of Vitalik's blog posts, titled "On Silos."[2]

Over the next several months, and up to this day, we became reverse mentors. He taught me a lot about blockchains, and I advised him on business matters and growing Ethereum. I may never comprehend a fraction of Vitalik's blockchain dreams on a given night, but one thing I am certain about, is that Vitalik Buterin is emerging as a savvy business person, following the ranks of other bright technologists, while continuing to lead the Ethereum core technology and its Foundation.

I proceeded to write 50 blog posts on Bitcoin, blockchains, and Ethereum, and immersed myself with global creators, innovators, pioneers, leaders, entrepreneurs, startups, enterprise executives and practitioners who were at the leading edges of blockchain technology and its implementation.

Much of this book is marked by the historical perspective I hold, which is based on 34 years of experience in the technology sector. The first phase of this journey included 14 formative years at Hewlett-Packard, followed by a second phase of 10 years as an independent consultant, author and influencer in the Internet space (1995–2005). In 1996, I authored one of the first business books on Internet business strategy, *Opening Digital Markets*,

allowing me to exhaustively analyze the significance of the Web on business, and work with small and large companies who were implementing it. In 2005, I learned how to become a professional analyst at Aberdeen Group, then followed that stint by three years at Cognizant Technology Solutions, where I became exposed to the true meanings of a borderless organization, with global arbitrage at the center of it. In 2008, and for another five years, I dived into the startup world as a founder of two mildly successful startups (Eqentia, and Engagio). They say you learn as much from failures as from successes.

My passion for the blockchain's peer-to-peer (P2P) technology was not a coincidence. In 2001, I had launched PeerIntelligence.com, a site that chronicled the first wave of P2P technologies. During this time, P2P was primarily about file sharing, and I gained an early appreciation of the power of this new technology. Sadly, these first attempts at P2P died on the vine, after legal assaults killed Napster, but in return, we gained the BitTorrent protocol as its valiant remnant.

All these experiences helped shape my thoughts about the blockchain, and influenced the preparation of this book.

In 2013, when I discovered Bitcoin and the world of blockchains, it brought me back to the early excitement of 1995, when some of us knew that the Internet was going to be transformational, coupled with flash backs about the early P2P days of 2001. Luckily, P2P was getting a shot in the arm in 2009 when the Bitcoin blockchain took its first breath.

When I was first exposed to the blockchain, I was reminded of Andy Grove's words in his 1996 book, *Only the Paranoid Survive*. He wrote, "*There's wind and then there's a typhoon. In this business you always have winds. But a 10x force is a change in an element of one's business of typhoon force.*" Of course, Andy was talking about the Internet, as a typhoon force that fundamentally alters one's business. Today, the blockchain is that 10x typhoon

force that is going to alter many businesses, and the journey is just starting.

I will admit that I went through great pains trying to understand the many facets of the blockchain. Many of its smart visionaries were technically inclined people who didn't focus on succinctly explaining its business implications, or intersections. My early quest to understand the blockchain required a lot of teeth pulling and tea leaves reading to connect the dots and find clarity. It was an agonizing encounter, and the source of my impetus for writing this book. I was determined to make it less dreadful for the rest of us to understand this technology and its ramifications.

The blockchain is part of the history of the Internet. It is at the same level as the World Wide Web in terms of importance, and arguably might give us back the Internet, in the way it was supposed to be: more decentralized, more open, more secure, more private, more equitable, and more accessible. Ironically, many blockchain applications also have a shot at replacing legacy Web applications, at the same time as they will replace legacy businesses that cannot loosen their grips on heavy-handed centrally enforced trust functions.

No matter how it unfolds, the blockchain's history will continue to be written well after you finish reading this book, just as the history of the Web continued to be written well after its initial invention. But here's what will make the blockchain's future even more interesting: you are part of it.

I hope that readers will find *The Business Blockchain* as useful as I found it exhilarating to write.

William Mougayar
Toronto, Ontario
wmougayar@gmail.com

MARCH 2016

NOTES

1. "A Next-Generation Smart Contract and Decentralized Application Platform," https://github.com/ethereum/wiki/wiki/White-Paper#ethereum.
2. "On Silos," https://blog.ethereum.org/2014/12/31/silos/.